Guía Paso a Paso para Implementar la Confidencialidad, Integridad y Disponibilidad en Correos Electrónicos mediante Firmas Digitales en Linux (Debian) y Windows

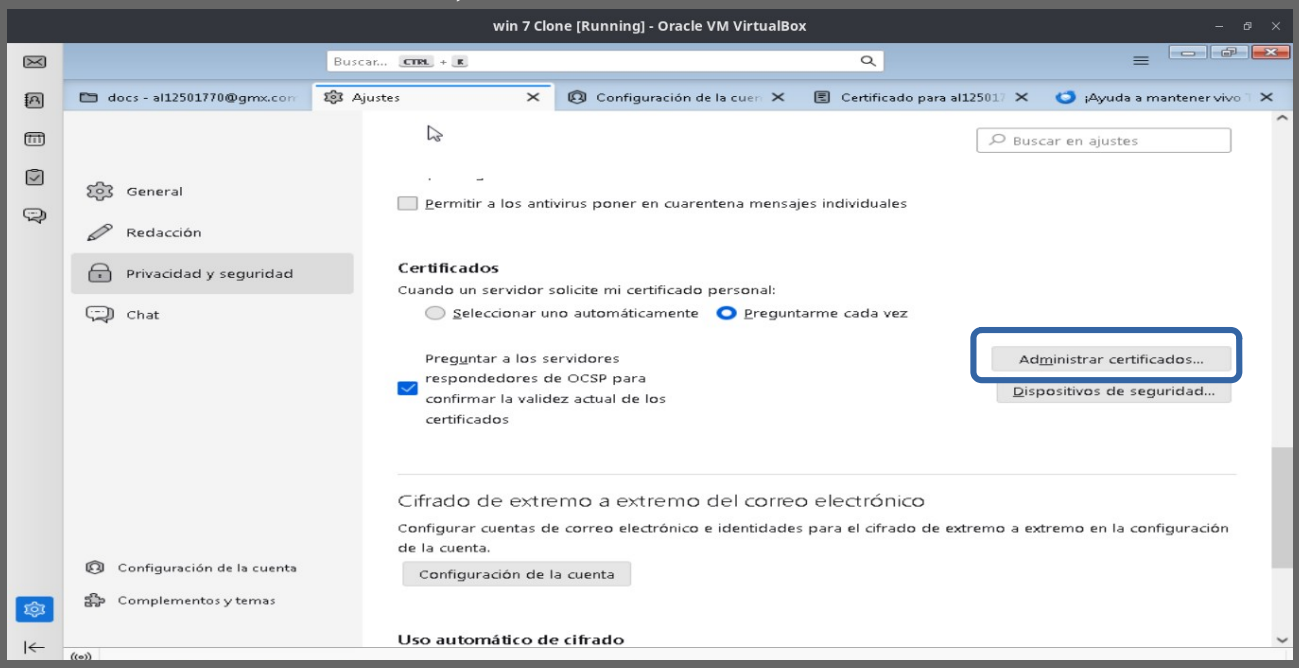
¿Quieres aprender más sobre soporte técnico y otros temas?
WWW.HAKATU.COM
Aprende a resolver problemas comunes y mucho más.

Ejercicio 2: Usar firmas digitales para correos

Objetivo: Asegurar que los correos electrónicos no han sido modificados. Este ejercicio básico tiene como objetivo enseñar cómo asegurar que los correos electrónicos no han sido modificados, mediante la implementación de firmas digitales utilizando herramientas en Linux (Debian) y Windows. A través de pasos prácticos, aprenderás a usar un certificado digital para firmar y verificar correos electrónicos, fortaleciendo tus conocimientos en ciberseguridad, según los estándares de CompTIA Security+.

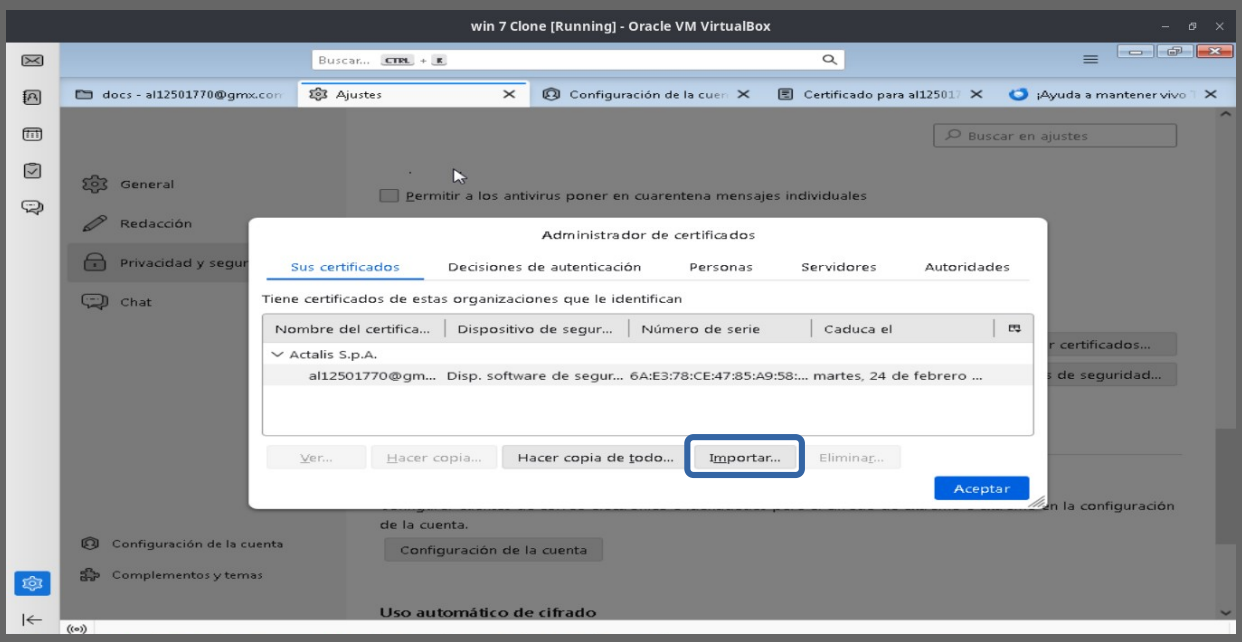
Paso a paso:

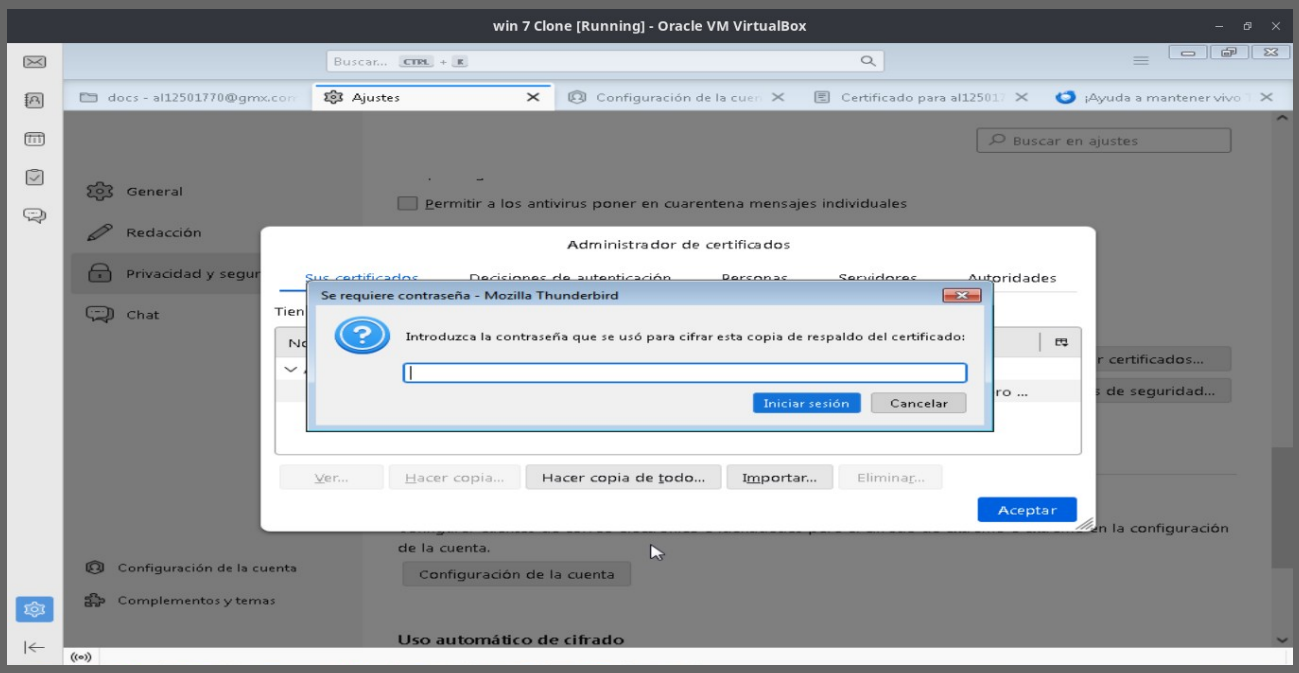
1. Obtener un certificado digital gratuito:
   • Debes obtener un certificado digital S/MIME, que permite firmar digitalmente los correos electrónicos.
   • Puedes obtener uno gratis en www.actalis.com, válido para una sola cuenta de correo.
   • Durante el proceso de registro, se generará un archivo .p12, que contiene:
   ◦ Clave privada: Se usa para firmar los correos.
   ◦ Clave pública: Permite a los destinatarios verificar la firma.
   ◦ Firma digital: Contiene el hash del mensaje cifrado con la clave privada.
2. Configurar el certificado en Thunderbird
   • Abre Thunderbird y ve a Menú > Configuración(engrane) > Privacidad y seguridad.
   • En la sección Certificados, haz clic en Administrador de certificados.



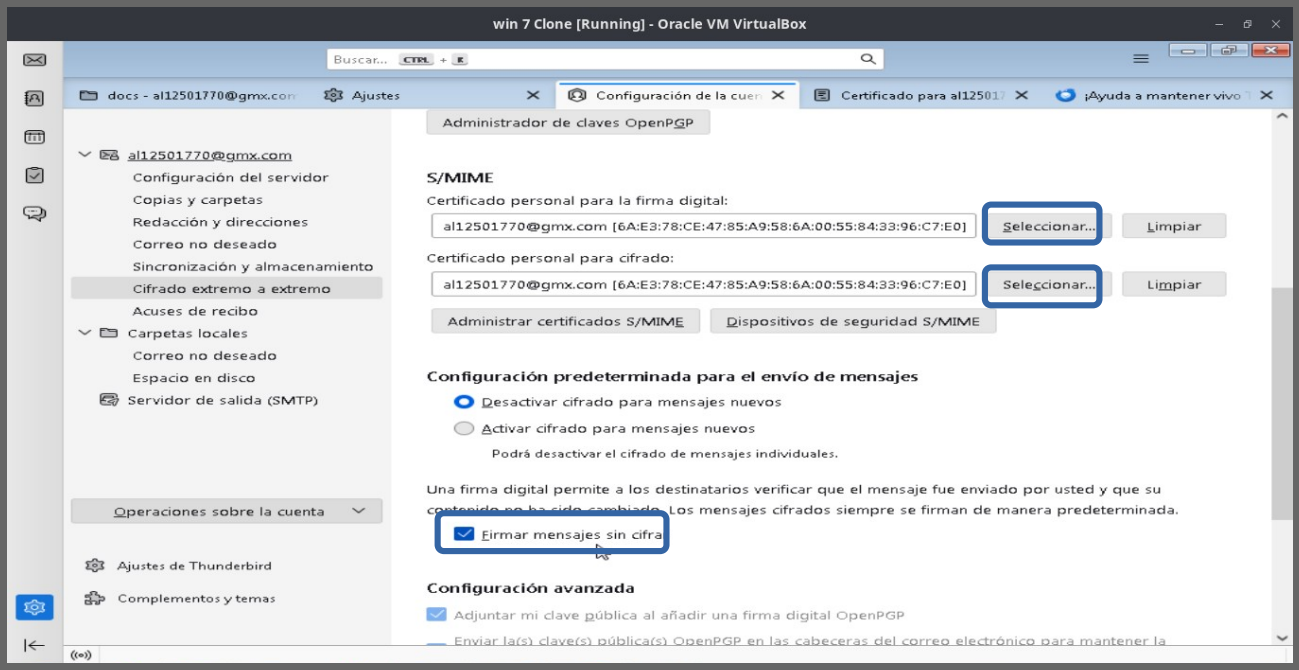
   • Importa el archivo .p12 usando la opción Importar.
   • Se te pedirá la contraseña que configuraste al obtener el certificado la que se te envio al correo.

¿Quieres aprender más sobre soporte técnico y otros temas?
WWW.HAKATU.COM
Aprende a resolver problemas comunes y mucho más.



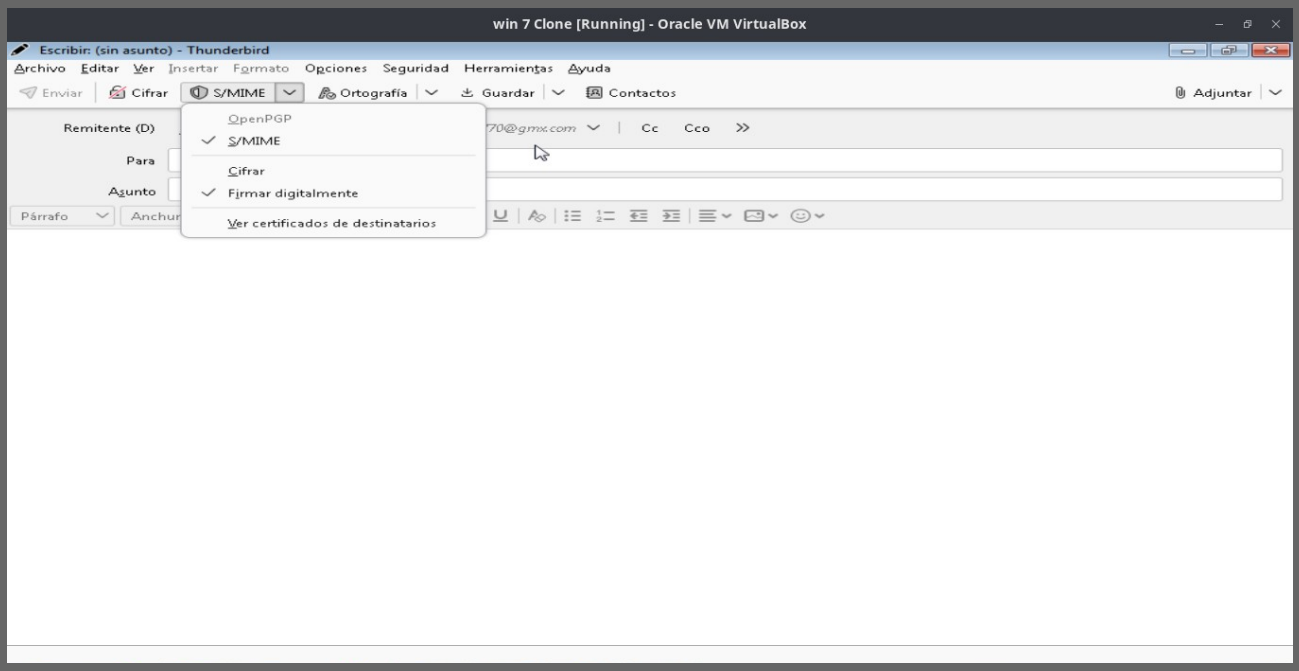


3. Habilitar la firma digital en los correos:
   - Ve a Configuración de la cuenta.
   - Selecciona Cifrado de extremo a extremo.
   - En la opción Firma digital (S/MIME), elige el certificado importado.
   - Activa la casilla Firmar digitalmente los mensajes salientes por defecto.



Estas opciones las puedes cambiar en el momento que redactas el correo.

4. Firmar manualmente un correo en Thunderbird:
   • Al redactar un correo, haz clic en Opciones > Seguridad.
   • Activa Firmar digitalmente este mensaje.
   • Cuando envíes el correo, Thunderbird generará un hash del mensaje, lo cifrará con tu clave privada y lo adjuntará como la firma digital.



¿Quieres aprender más sobre soporte técnico y otros temas?
WWW.HAKATU.COM
Aprende a resolver problemas comunes y mucho más.

5. Verificar la firma digital en un correo recibido:
   • Cuando un destinatario reciba tu correo, su cliente de correo intentará validar la firma digital usando tu clave pública (adjunta en el certificado).
   • El cliente comparará el hash del mensaje original con el hash descifrado de la firma.
   • Si coinciden, el correo no ha sido alterado y proviene realmente de ti.

6. Restricciones y validaciones en este ejercicio:

   • Los servicios de correo web (Gmail, Outlook Web, etc.) no validan firmas digitales. Se requiere un cliente de correo como Thunderbird u Outlook.

   • Thunderbird validará automáticamente la autenticidad del certificado verificando que:

   ◦ No haya sido revocado.

   ◦ Se encuentre dentro de su periodo de vigencia.

7. Para extraer la clave pública del certificado desde el archivo .p12 descargado de www.actalis.com y validar la firma sin un cliente de correo, puedes usar OpenSSL con los siguientes comandos:

   ```
   openssl pkcs12 -in certificado.p12 -clcerts -nokeys -out certificado_publico.cert
   ```

   • El certificado público extraído del archivo `.p12` generalmente se guarda con la extensión `.cert` o `.crt`, dependiendo del formato deseado. Para enviarlo al receptor, se suele utilizar el formato `.cert` o `.crt`, ya que son reconocidos por la mayoría de los clientes de correo y sistemas operativos.

8. **Paso 8: Validar la firma digital en un correo autofirmado**

- Envíate un correo firmado digitalmente a ti mismo.
- Abre el correo en un cliente de correo compatible como **Thunderbird o Outlook**.
- **Sin importar si tienes el certificado público:**
  - El cliente de correo intentará validar la firma automáticamente.
  - Si el certificado público no está en tu lista de certificados de confianza, recibirás una advertencia de que la firma no puede ser verificada.
- **Si importas el certificado público (.cert o .crt):**
  - El cliente reconocerá la firma como válida.
  - Thunderbird y Outlook mostrarán un ícono o mensaje indicando que el correo es auténtico.

Puntos clave sobre la validación de firmas digitales en correos electrónicos:

✅ Solo los clientes de correo instalados en la máquina pueden validar firmas digitales.

❌ Los servicios de correo web NO validan firmas digitales (ni Gmail, ni Outlook Web, ni Yahoo Mail).

✅ Para que la firma sea válida, el certificado no debe estar expirado ni revocado.

✅ La validación solo ocurre si el cliente de correo reconoce el certificado del remitente.

Consejo: Las firmas digitales permiten asegurar la autenticidad y la integridad de los correos electrónicos, ayudando a evitar fraudes o suplantaciones de identidad.